UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,102	12/02/2003	Masato Yamamichi	2003_1742A	5711

52349 7590 07/17/2007

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/725,102	YAMAMICHI ET AL.	
	Examiner	Art Unit	
	Oscar A. Louie	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47,49 and 50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47,49 and 50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 04/19/2007. The examiner notes that the amendments to the specification and the cancellation of Claims 48 & 51 have been acknowledged. It is also noted that the amendments to Claims 47 & 50 have over come the 35 U.S.C. 101 rejections, thus are withdrawn. Claims 1-47, 49, & 50 are pending and have been considered as follows.

Specification

1. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

- Pages 11 & 172 contain embedded hyperlinks in lines 1, 9-10 of page 11 and line 9 of page 172.

Claim Objections

2. Claim 26 is objected to because of the following informalities: Claim 26 discloses, "the public-key encryption algorithm an the public-key decryption algorithm confirm to an NTRU cryptosystem." The term "confirm" is interpreted by the examiner as being a typographical error and will be read as "conform." Appropriate correction is required.

Double Patenting

3. Claims 1-12, 14-32, & 36-51 of this application conflict with claims 1-7, 9-33, 37-40, & 43 of Application No. 10/725208. 37 CFR 1.78(b) provides that when two or more applications filed by the same applicant contain conflicting claims, elimination of such claims from all but one application may be required in the absence of good and sufficient reason for their retention during pendency in more than one application. Applicant is required to either cancel the conflicting claims from all but one application or maintain a clear line of demarcation between the applications. See MPEP § 822.

Claim 1:

- Claim 1 of Application No. 10/725208 discloses a key agreement system comprising equivalent elements as Claim 1 of Application No. 10/725102. The features disclosed as two elements in Claim 1 of Application No. 10/725208 as, "a first encryption unit," and, "second encryption unit," are equivalent to, "an encryption unit," which is disclosed as a single element by Claim 1 of Application No. 10/725102.

Claim 2:

- Claim 2 of Application No. 10/725208 discloses equivalent elements to Claim 2 of Application No. 10/725102.

Claim 3:

- Claim 3 of Application No. 10/725102 discloses a shared-key generation apparatus for use in the system as in Claim 1 above, and comprises of equivalent elements as Claim 3

of Application No. 10/725208. The features disclosed as two elements in Claim 3 of Application No. 10/725102 as, "a first encryption unit," and, "second encryption unit," are equivalent to, "an encryption unit," which is disclosed as a single element by Claim 3 of Application No. 10/725208.

Claim 4:

- Claim 4 of Application No. 10/725102 and Claim 16 of Application No. 10/725208, disclose equivalent elements.

Claim 5:

- Claim 5 of Application No. 10/725102 and Claims 7 & 17 of Application No. 10/725208, disclose equivalent elements. Claim 4 of Application No. 10/725208 discloses, "the shared-key generating unit performs a one-way function on the seed value, to generate the functional value, and generates the blind value and the shared key from the functional value," which is equivalent to Claim 5 of Application No. 10/725102.

Claims 6, 18, 32, & 38:

- Claims 6, 18, 32, & 38 of Application No. 10/725102 and Claims 8 & 18 of Application No. 10/725208, disclose equivalent elements.

Claims 7 & 39:

- Claim 19 of Application No. 10/725208 discloses elements equivalent to Claims 7 & 39 of Application No. 10/725102.

Claim 8:

- Claim 8 of Application No. 10/725102 and Claim 17 of Application No. 10/725208, disclose equivalent elements. Claim 10 of Application No. 10/725208 discloses, "the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates a verification value, the blind value, and the shared key," which is equivalent to Claim 8 of Application No. 10/725102.

Claims 9 & 11:

- Claims 4, 6, & 10 of Application No. 10/725208 disclose, "a public-key obtaining subunit operable to obtain a public key; and a public-key encryption subunit operable to perform a public-key encryption algorithm on the seed value, using the public key and the blind value, to generate an encryption seed value as the encryption information," and, a public-key obtaining subunit operable to obtain a public key; a public-key encryption subunit operable to generate a blind value, perform the public-key encryption algorithm on the seed value using the public key and the blind value, to generate a public-key cipher text," and, "a public-key obtaining subunit operable to obtain a public key; a first encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate a first cipher text," which is equivalent to Claims 9 & 11 of Application No. 10/725102.

Claims 10 & 12:

- Claims 5, 9, & 11 of Application No. 10/725208 disclose, "the public-key encryption algorithm conforms to an NTRU cryptosystem," and, "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of

NTRU cryptosystem, as the public key," and, "the public-key encryption subunit generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, and encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed value polynomial as the encryption seed value," which is equivalent to Claims 10 & 12 of Application No. 10/725102.

Claims 14, 22, 28, & 36:

- Claim 13 of Application No. 10/725208 discloses, "the different computation algorithm is bitwise exclusive-or, and the second encryption subunit performs the bitwise exclusive-or on the verification value and the seed value, to generate the second cipher text," which is equivalent to Claims 14, 22, 28, & 36 of Application No. 10/725102.

Claims 15 & 29:

- Claim 12 of Application No. 10/725208 discloses, "the different computation algorithm is a symmetric key encryption algorithm, and the second encryption subunit performs the symmetric key encryption algorithm on the seed value using the verification value as a key, to generate the second cipher text," which is equivalent to Claims 15 & 29 of Application No. 10/725102.

Claims 16 & 30:

- Claim 14 of Application No. 10/725208 discloses, "the different computation algorithm is addition, and the second encryption subunit performs the addition on the verification value and the seed value, to generate the second cipher text," which is equivalent to Claims 16 & 30 of Application No. 10/725102.

Claims 17 & 31:

- Claim 15 of Application No. 10/725208 discloses, "the different computation algorithm is multiplication, and the second encryption subunit performs the multiplication on the verification value and the seed value, to generate the second cipher text," which is equivalent to Claims 17 & 31 of Application No. 10/725102.

Claims 19, 20, & 21:

- Claim 10 of Application No. 10/725208 discloses, "the encryption unit generates the encryption information that includes the first cipher text and the second cipher text," which is equivalent to Claims 19, 20, & 21 of Application No. 10/725102.

Claim 23:

- Claim 22 of Application No. 10/725208 discloses equivalent elements as Claim 23 of Application No. 10/725102.

Claim 24:

- Claim 24 of Application No. 10/725102 discloses a shared-key recovery apparatus comprising equivalent elements as Claim 21 of Application No. 10/725208. The features disclosed in Claim 24 of Application No. 10/725102 as, "a first decryption unit operable to decrypt the first encryption information, to generate a first decryption verification

value; a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value," are equivalent to, "a decryption unit operable to decrypt the encryption information, to generate a decryption seed value," as disclosed by Application No. 10/725208.

Claim 25:

- Claim 22 of Application No. 10/725208 discloses, "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates the blind value and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the seed value using the public key and the blind value, to generate an encryption seed value as the encryption information, and transmits the encryption seed value," and, "a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key; and a public-key decryption subunit operable to perform, on the received encryption seed value, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, using the obtained secret key, to generate the decryption seed value," which is equivalent to Claim 25 of Application No. 10/725102.

Claim 26:

- Claims 23 & 27 of Application No. 10/725208 disclose elements equivalent to Claim 26 of Application No. 10/725102.

Claim 27:

- Claim 25 of Application No. 10/725208 discloses elements equivalent to Claim 27 of Application No. 10/725102.

Claim 37:

- Claim 22 of Application No. 10/725208 discloses, "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates the blind value and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the seed value using the public key and the blind value, to generate an encryption seed value as the encryption information, and transmits the encryption seed value," and, "the shared-key generating unit performs the one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption blind value and the decryption shared key from the decryption functional value," which is equivalent to Claim 37 of Application No. 10/725102.

Claim 40:

- Claim 28 of Application No. 10/725208 discloses, "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates a verification value, the blind value, and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the verification value using the public key and the blind value to generate a first cipher text, performs, based on the verification value, a computation algorithm different from the public-key encryption algorithm on the seed value, to generate a second cipher text, generates the encryption information that includes the first cipher text and the second cipher text, and transmits the encryption information," which is equivalent to Claim 40 of Application No. 10/725102.

Claim 41:

- Claim 24 of Application No. 10/725208 discloses, "the shared-key generation apparatus obtains a public key, generates a blind value, performs a public-key encryption algorithm on the seed value using the public key and the blind value to generate a public-key cipher text, performs a second one-way function on at least one of the seed value, the blind value, and the shared key to generate a second functional value, generates the encryption information that includes the public-key cipher text and the second functional value, and transmits the encryption information," which is equivalent to the disclosure of Claim 41 of Application No. 10/725102, "the shared-key generation apparatus obtains a public key, performs a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information."
- Claim 10 of Application No. 10/725208 discloses, "a public-key obtaining subunit operable to obtain the public key," which is equivalent to the disclosure of Claim 41 of Application No. 10/725102, "a public-key obtaining subunit operable to obtain the public key."
- Claim 21 of Application No. 10/725208 discloses, "a re-encryption unit operable to encrypt the decryption seed value based on the decryption blind value, to generate re-encryption information; a judging unit operable to judge, based on the encryption information and there-encryption information, whether the decryption shared key should be outputted," which is equivalent to the disclosure of Claim 41 of Application No. 10/725102, "a re-encryption subunit operable to perform the public-key encryption algorithm on one of the first decryption verification value and the second decryption

verification value, using the public key and the decryption blind value, to generate re-encryption information; and a judging subunit operable to judge, based on the first encryption information and the re-encryption information, whether the decryption shared key should be outputted or not."

Claims 42 & 44:

- Claim 29 of Application No. 10/725208 discloses, "the judging unit judges whether the encryption verification-value polynomial as the first cipher text is identical to the re-encryption verification-value polynomial as the re-encryption information," which is equivalent to Claims 42 & 44 of Application No. 10/725102.

Claim 43:

- Claim 29 of Application No. 10/725208 discloses, "the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem," and, "the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate an encryption verification-value polynomial as the first cipher text, generates the encryption information that includes the encryption verification-value polynomial as the first cipher text and the second cipher text, and transmits the encryption information," and, "the public-key obtaining subunit obtains the public-key

polynomial," and, "the re-encryption subunit generates a decryption verification-value polynomial from the decryption verification value, generates a blind-value polynomial from the decryption blind value, and encrypts the decryption verification-value polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the decryption verification-value polynomial, to generate a re-encryption verification-value polynomial as the re-encryption information," which is equivalent to Claim 43 of Application No. 10/725102.

Claim 45:

- Claim 37 of Application No. 10/725208 discloses, "the shared-key generation apparatus further obtains a content, encrypts the obtained content using the shared key to generate an encrypted content, and transmits the encrypted content, and the shared-key recovery apparatus further includes: a content receiving unit operable to receive the encrypted content; a decryption unit operable to decrypt the received encrypted content using the outputted decryption shared key, to generate a decrypted content; and a playback unit operable to playback the decrypted content," which is equivalent to Claim 45 of Application No. 10/725102.

Claim 46:

- Claim 38 of Application No. 10/725208 discloses, "a seed-value generating step of generating a seed value; a shared-key generating step of generating a blind value and a

shared key, from the seed value; an encryption step of encrypting the seed value based on the blind value, to generate encryption information; and a transmitting step of transmitting the encryption information," which is equivalent to Claim 46 of Application No. 10/725102.

Claim 47:

- Claim 39 of Application No. 10/725208 discloses, "a seed-value generating step of generating a seed value; a shared-key generating step of generating a blind value and a shared key, from the seed value; an encryption step of encrypting the seed value based on the blind value, to generate encryption information; and a transmitting step of transmitting the encryption information," which is equivalent to Claim 47 of Application No. 10/725102.

Claim 49:

- Claim 41 of Application No. 10/725208 discloses, "a receiving step of receiving the encryption information," and, "a decryption step of decrypting the encryption information, to generate a decryption seed value," and, "a shared-key generating step of generating a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus," and, "a judging step of judging, based on the encryption information and there-encryption information, whether the decryption shared key should be outputted," and, "an outputting step, when the judging unit has judged affirmatively, of outputting the decryption shared key," which is equivalent to Claim 49 of Application No. 10/725102.

Claim 50:

- Claim 42 of Application No. 10/725208 discloses, "a receiving step of receiving the encryption information," and, "a decryption step of decrypting the encryption information, to generate a decryption seed value," and, "a shared- key generating step of generating a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus," and, "a judging step of judging, based on the encryption information and there-encryption information, whether the decryption shared key should be outputted," and, "an outputting step, when the judging unit has judged affirmatively, of outputting the decryption shared key," which is equivalent to Claim 50 of Application No. 10/725102.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-15, 18-29, 32-46, 47, 49, & 50 are rejected under 35 U.S.C. 102(b) as being anticipated by Hoffstein (WO-9808323-A1).

Claim 1:

Hoffstein discloses a key agreement system as in Claim 1 of the applicant comprising,

- "the key creator, call him Dan..." and the equations or formulas which disclose the system functions of, "a seed- value generating unit operable to generate a seed value," and "a first shared-key generating unit operable to generate a verification value and a shared key, from the seed value" [pages 13-15].
- "the encoder, call her Cathy..." and the equations or formulas which disclose the system functions of, "a first encryption unit operable to encrypt the verification value to generate first encryption information; a second encryption unit operable to encrypt the seed value based on the verification value, to generate second encryption information" [page 16].
- "Communication is via transceiver" (i.e. "a transmitting unit operable to transmit the first encryption information and the second encryption information") [page 8 lines 22-24].
- Fig 5 (i.e. "a receiving unit operable to receive the first encryption information and the second encryption information") [Fig 5 Box# 530].
- "Dan..." and the equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a first decryption unit operable to decrypt the first encryption information, to generate a first decryption verification value; a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value") [pages 17-18].
- "Dan..." and the equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a second shared-key generating unit operable to generate a second decryption verification

value and a decryption shared key, from the decryption seed value and according to a same method as used in the first shared-key generating unit") [pages 18-19].

- Fig 6 ("i.e. a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted") [Fig 6 Box# 640].
- "The block 210 represents the generating of the public and private key information, and the 'publishing' of the public key" ("i.e. "an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key") [page 22 lines 7-9 & 12-23].

Claim 2:

Hoffstein discloses a key agreement system as in Claim 1 above further comprising,

- Fig 4 ("i.e. an obtaining unit operable to obtain a content") [Fig 4 Box# 420].
- "The encoding technique of an embodiment of the public key cryptosystem hereof uses a mixing system based on polynomial algebra and reduction modulo two numbers, p and q, while the decoding technique uses an unmixing system whose validity depends on the elementary probability theory" (i.e. "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content") [page 9].
- "Communication is via transceiver..." (i.e. "the transmitting unit further transmits the encrypted content") [page 8 lines 22-24].
- Fig 5 (i.e. "the receiving unit further receives the encrypted content") [Fig 5 Box# 530].

- "The decoding for this matrix example is described next..." (i.e. "a decryption unit operable to decrypt the received encrypted content using the decryption shared key, to generate a decrypted content") [page 20].
- "Finally Dan computes...to recover the original message m." (i.e. "an outputting unit operable to output the decrypted content" [page 20].

Claim 3:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 1 above comprising,

- "the key creator, call him Dan..." and the equations or formulas which disclose the system functions of, (i.e. "a seed-value generating unit operable to generate a seed value," and, "a shared-key generating unit operable to generate a verification value and a shared key, from the seed value") [page 15].
- "the encoder, call her Cathy..." and the equations or formulas which disclose the system functions of, "a first encryption unit operable to encrypt the verification value to generate first encryption information; a second encryption unit operable to encrypt the seed value based on the verification value, to generate second encryption information" [page 16].
- "Communication is via transceiver" (i.e. "a transmitting unit operable to transmit the first encryption information and the second encryption information") [page 8 lines 22-24].

Claim 4:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,

- "...choose integer parameters N, K, p, and q... " and the referenced equations or formulas which disclose the system functions of, (i.e. "the seed-value generating unit generates a random number, as the seed value") [pages 13-14].

Claim 5:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,.

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula" (i.e. "the shared-key generating unit performs a one-way function on the seed value to generate a functional value, and generates the verification value and the shared key from the functional value") [pages 16-17].

Claim 6:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 5 above further comprising,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula" (i.e. "the shared-key generating unit performs, on the seed value, a hash function as the one-way function, to generate the functional value") [pages 16-17].

Claim 7:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 5 above further comprising,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula" (i.e. "the shared-key generating unit generates the verification value by setting a part of the functional value as the verification value, and generates the shared key by setting another part of the functional value as the shared key") [pages 16-17].

Claim 8:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula" (i.e. "the shared-key generating unit performs a one-way function on the seed value to generate a functional value, and generates the verification value, the shared key, and a blind value, from the functional value") [pages 16-17].

Claim 9:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 8 above further comprising,

- "The public key information can be published; that is, made available to any member of the public or to any desired group..." (i.e. "a public-key obtaining subunit operable to obtain a public key") [page 22 lines 12-23].

- "The block 220 represents the routine that can be used by the message sender to encode the plaintext message using the public key of the intended message recipient." (i.e. "a public-key encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information") [page 22 lines 24-27 & page 23 lines 1-4].

Claim 10:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 9 above further comprising,

- "1.2 Key Creation. To create an NTRU key," (i.e. "the public-key encryption algorithm conforms to an NTRU cryptosystem") [page 31].
- "Dan randomly chooses...The polynomial f must satisfy the additional requirement... Dan next computes the quantities... Dan's public key is the list of polynomials... Dan's private key is the single polynomial f..." (i.e. "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key,") [page 31].
- "1.2 Key Creation...1.3 Encoding..." (i.e. "the public-key encryption subunit generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial") [page 31].

Claim 11:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,

- "The public key information can be published; that is, made available to any member of the public or to any desired group..." (i.e. "a public-key obtaining subunit operable to obtain a public key," and,) [page 22 lines 12-23].
- "The block 220 represents the routine that can be used by the message sender to encode the plaintext message using the public key of the intended message recipient." (i.e. "a public-key encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key, to generate the first encryption information") [page 22 lines 24-27 & page 23 lines 1-4].

Claim 12:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 11 above further comprising,

- "1.2 Key Creation. To create an NTRU key," (i.e. "the public-key encryption algorithm conforms to an NTRU cryptosystem") [page 31].
- "1.2 Key Creation...1.3 Encoding..." (i.e. "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key") [page 31].
- "1.2 Key Creation...1.3 Encoding..." (i.e. "the public-key encryption subunit generates a verification-value polynomial from the verification value, generates a blind value, generates a blind-value polynomial from the blind value, and encrypts the verification-

value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial") [page 31].

Claim 13:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula" (i.e. "the second encryption unit performs a one-way function on the verification value to generate a functional value, and performs an encryption algorithm, on the seed value, using the functional value, to generate the second encryption information") [pages 16-17].

Claim 14:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 13 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the second encryption unit performs bitwise exclusive-or as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information") [pages 16-17].

Claim 15:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 13 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the second encryption unit performs a symmetric key encryption algorithm as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information") [pages 16-17].

Claim 18:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 13 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the second encryption unit performs, on the verification value, a hash function as the one-way function, to generate the functional value") [pages 16-17].

Claim 19:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 13 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the second encryption unit performs an encryption algorithm on the seed value using the verification value, to generate the second encryption information") [pages 16-17].

Claim 20:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 13 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the second encryption unit encrypts the seed value using the verification value and the first encryption information") [pages 16-17].

Claim 21:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 13 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the second encryption unit performs a one-way function on the verification value and the first encryption information, to generate the functional value, and performs an encryption algorithm on the seed value using the functional value, to generate the second encryption information") [pages 16-17].

Claim 22:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 13 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the second encryption unit performs bitwise exclusive-or as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information") [pages 16-17].

Claim 23:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,

- Fig 4 (i.e. "an obtaining unit operable to obtain a content") [Fig 4 Box# 420].
- "The encoding technique of an embodiment of the public key cryptosystem hereof uses a mixing system based on polynomial algebra and reduction modulo two numbers, p and q, while the decoding technique uses an unmixing system whose validity depends on the elementary probability theory" (i.e. "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content") [page 9].
- "Communication is via transceiver" (i.e. "the transmitting unit further transmits the encrypted content") [page 8 lines 22-24].

Claim 24:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 1 above comprising,

- Fig 5 (i.e. "a receiving unit operable to receive the first encryption information and the second encryption information") [Fig 5 Box# 530].
- "Dan..." and the equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a first decryption unit operable to decrypt the first encryption information, to generate a first decryption verification value; a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value") [pages 17-18].

- "the key creator, call him Dan..." and the equations or formulas which disclose the system functions of, (i.e. "a shared-key generating unit operable to generate a second decryption verification value and a decryption shared key, from the decryption seed value and according to a same method as used in the shared-key generation apparatus") [pages 14-15].
- Fig 6 (i.e. "a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted") [Fig 6 Box# 640].
- "The block 210 represents the generating of the public and private key information, and the 'publishing' of the public key" (i.e. "an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key") [page 22 lines 7-9 & 12-23].

Claim 25:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 24 above further comprising,

- "1.2 Key Creation...1.3 Encoding" (i.e. "the shared-key generation apparatus obtains a public key, and performs a public-key encryption algorithm on the verification value, using the public key, to generate the first encryption information," and, "a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key," and,

"a public-key decryption subunit operable to perform a public-key decryption algorithm on the first encryption information, to generate the first decryption verification value, the public-key decryption algorithm corresponding to the public-key encryption algorithm") [page 31].

Claim 26:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 25 above further comprising,

- "1.2 Key Creation...1.3 Encoding...1.4 Decoding..." (i.e. "the public-key encryption algorithm and the public-key decryption algorithm confirm to an NTRU cryptosystem," and, "the shared-key generation apparatus obtains, as the public key, a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, generates a verification-value polynomial from the verification value, generates a blind value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial," and, "the receiving unit receives the first encryption information as a polynomial," and, "the secret-key obtaining subunit obtains, as the secret key, a secret-key polynomial generated according to the key generation algorithm of the NTRU cryptosystem," and "the public-key subunit decrypts the first encryption information as a polynomial, according to a decryption algorithm corresponding to the NTRU cryptosystem's encryption algorithm, using the secret-key

polynomial as a key, to generate a decryption verification-value polynomial, and generates the first decryption verification value from the decryption verification-value polynomial.") [page 31].

Claim 27:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 24 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs a one-way function on the verification value, to generate a functional value, and performs an encryption algorithm on the seed value using the functional value, to generate the second encryption information," and, "the second decryption unit performs the one-way function on the first decryption verification value, to generate a decryption functional value, and performs, on the second encryption information, a decryption algorithm corresponding to the encryption algorithm, using the decryption functional value, to generate the decryption seed value") [pages 16-17].

Claim 28:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 27 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs, on the functional value and the seed value, bitwise

exclusive-or as the encryption algorithm, to generate the second encryption information, and the second decryption unit performs, on the decryption functional value and the second encryption information, bitwise exclusive-or as the decryption algorithm, to generate the decryption seed value") [pages 16-17].

Claim 29:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 27 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs, on the functional value and the seed value, a symmetric key encryption algorithm as the encryption algorithm, to generate the second encryption information, and the second decryption unit performs, on the decryption functional value and the second encryption information, a symmetric key decryption algorithm as the decryption algorithm, to generate the decryption seed value, the symmetric key decryption algorithm corresponding to the symmetric key encryption algorithm.") [pages 16-17].

Claim 32:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 27 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs, on the verification value, a hash function as the one-way

function, to generate the functional value, and the second decryption unit performs, on the first decryption verification value, the hash function as the one-way function, to generate the decryption functional value" [pages 16-17].

Claim 33:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 24 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs an encryption algorithm on the seed value using the verification value, to generate the second encryption information, and the second decryption unit performs a decryption algorithm corresponding to the encryption algorithm, on the second encryption information using the first decryption verification value, to generate the decryption seed value" [pages 16-17].

Claim 34:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 24 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus encrypts the seed value using the verification value and the first encryption information, and the second decryption unit decrypts the second encryption information, using the first decryption verification value and the first encryption information, to generate the decryption seed value" [pages 16-17].

Claim 35:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 34 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs a one-way function on the verification value and the first encryption information, to generate a functional value, and performs an encryption algorithm on the seed value using the functional value, to generate the second encryption information, and the second decryption unit performs the one-way function on the first decryption verification value and the first encryption information, to generate a decryption functional value, and performs a decryption algorithm corresponding to the encryption algorithm, on the second encryption information, using the decryption functional value, to generate the decryption seed value" [pages 16-17].

Claim 36:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 35 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs bitwise exclusive-or as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information, and the second decryption unit performs bitwise exclusive-or as the decryption algorithm, on the decryption functional value and the second encryption information, to generate the decryption seed value" [pages 16-17].

Claim 37:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 24 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs a one-way function on the seed value, to generate a functional value, and generates the verification value and the shared key from the functional value, and the shared-key generating unit performs the one-way function on the decryption seed value, to generate a decryption functional value, and generates the second decryption verification value and the decryption shared key from the decryption functional value" [pages 16-17].

Claim 38:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 37 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs, on the seed value, a hash function as the one-way function, to generate the functional value, and the shared-key generating unit performs, on the decryption seed value, the hash function as the one-way function, to generate the decryption functional value" [pages 16-17].

Claim 39:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 37 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus generates the verification value by setting a part of the functional value as the verification value, and generates the shared key by setting another part of the functional value as the shared key, and the shared-key generating unit generates the second decryption verification value by setting a part of the decryption functional value as the second decryption verification value, and generates the decryption shared key by setting another part of the decryption functional value as the decryption shared key" [pages 16-17].

Claim 40:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 24 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs a one-way function on the seed value, to generate a functional value, generates the verification value, the shared key, and a blind value, from the functional value, obtains a public key, and performs a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate

the first encryption information, and the shared-key generating unit performs the one-way function on the decryption seed value, to generate a decryption functional value, and generates, from the decryption functional value, the second decryption verification value, the decryption shared key, and the decryption blind value" [pages 16-17].

Claim 41:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 40 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus obtains a public key, performs a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information," and, "a re-encryption subunit operable to perform the public-key encryption algorithm on one of the first decryption verification value and the second decryption verification value, using the public key and the decryption blind value, to generate re-encryption information" [pages 16-17].
- "The public key information can be published; that is, made available to any member of the public or to any desired group..." (i.e. "a public-key obtaining subunit operable to obtain the public key") [page 22 lines 12-23].
- Fig 6 (i.e. "a judging subunit operable to judge, based on the first encryption information and the re-encryption information, whether the decryption shared key should be outputted or not") [Fig 6 Box# 640].

Claim 42:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 41 above further comprising,

- "The decoding for this matrix example is described next..." (i.e. "the judging subunit compares the first encryption information and the re-encryption information, thereby judging that the decryption shared key should be outputted if the first encryption information is identical to the re-encryption information") [page 20].

Claim 43:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 41 above further comprising,

- "1.2 Key Creation...1.3 Encoding" (i.e. "the public-key encryption algorithm conforms to an NTRU cryptosystem, the shared-key generation apparatus obtains, as the public key, a public key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial") [page 31].
- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the public-key obtaining subunit obtains the public-key polynomial, and the re-encryption subunit generates a decryption verification-value polynomial from the second decryption

verification value, generates a decryption blind-value polynomial from the decryption blind value, and encrypts the decryption verification-value polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the decryption blind- value polynomial t o randomize t h e decryption verification-value polynomial, to generate the re- encryption information as a polynomial" [pages 16-17].

Claim 44:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 24 above further comprising,

- "The decoding for this matrix example is described next..." (i.e. "the judging unit compares the first decryption verification value and the second decryption verification value, thereby judging that the decryption shared key should be outputted if the first decryption verification value is identical to the second decryption verification value") [page 20].

Claim 45:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 24 above further comprising,

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus further obtains a content, encrypts the content using t h e shared key to generate an encrypted content, and transmits the encrypted content" [pages 16-17].
- Fig 5 (i.e. "the receiving unit further receives the encrypted content") [Fig 5 Box# 530].

- "The decoding for this matrix example is described next..." (i.e. "a decryption unit operable to decrypt the received encrypted content using t h e decryption shared key, to generate a decrypted content; and an outputting unit operable to output the decrypted content") [page 20].

Claim 46:

Hoffstein discloses a shared-key generation method used in the key agreement system as in Claim 1 above comprising,

- "the key creator, call him Dan..." and the equations or formulas which disclose the system functions of, "a seed-value generating step of generating a seed value; a shared-key generating step of generating a verification value and a shared key, from the seed value" [pages 13-15].
- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a first encryption step of encrypting the verification value to generate first encryption information; a second encryption step of encrypting the seed value based on the verification value, to generate second encryption information" [pages 16-17].
- "Communication is via transceiver" (i.e. "a transmitting step of transmitting the first encryption information and the second encryption information") [page 8 lines 22-24].

Claim 47:

Hoffstein discloses a shared-key generation program used in the key agreement system as in Claim 1 above comprising,

- "the key creator, call him Dan..." and the equations or formulas which disclose the system functions of, "a seed-value generating step of generating a seed value; a shared-

key generating step of generating a verification value and a shared key, from the seed value" [pages 13-15].

- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a first encryption step of encrypting the verification value to generate first encryption information; a second encryption step of encrypting the seed value based on the verification value, to generate second encryption information" [pages 16-17].
- "Communication is via transceiver" (i.e. "a transmitting step of transmitting the first encryption information and the second encryption information") [page 8 lines 22-24].

Claim 49:

Hoffstein discloses a shared-key recovery method used in the key agreement system as in Claim 1 above comprising,

- Fig 5 (i.e. "a receiving step of receiving the first encryption information and the second encryption information") [Fig 5 Box# 530].
- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a first decryption step of decrypting the first encryption information, to generate a first decryption verification value; a second decryption step of decrypting the second encryption information based on the first decryption verification value, to generate a decryption seed value; a shared-key generating step of generating a second decryption verification value and a decryption shared key, from the decryption seed value and according to a same method as used in the shared-key generation apparatus" [pages 16-17].
- "The decoding for this matrix example is described next..." (i.e. "a judging step of judging, based on the first decryption verification value and the second decryption

verification value, whether the decryption shared key should be outputted; and an outputting step, when the judging unit has judged affirmatively, of outputting the decryption shared key") [page 20].

Claim 50:

Hoffstein discloses a shared-key recovery program used in the key agreement system as in Claim 1 above comprising,

- Fig 5 (i.e. "a receiving step of receiving the first encryption information and the second encryption information") [Fig 5 Box# 530].
- The equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a first decryption step of decrypting the first encryption information, to generate a first decryption verification value; a second decryption step of decrypting the second encryption information based on the first decryption verification value, to generate a decryption seed value; a shared-key generating step of generating a second decryption verification value and a decryption shared key, from the decryption seed value and according to a same method as used in the shared-key generation apparatus" [pages 16-17].
- "The decoding for this matrix example is described next..." (i.e. "a judging step of judging, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted; and an outputting step, when the judging unit has judged affirmatively, of outputting the decryption shared key") [page 20].

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 16, 17, 30, & 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffstein (WO-9808323-A1).

Claims 16, 17, 30, & 31:

- Hoffstein discloses a key agreement system as in Claim 1 above, but does not explicitly disclose "the second encryption unit performs addition as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information," and, "the second encryption unit performs multiplication as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information," and, "the shared-key generation apparatus performs, on the functional value and the seed value, addition as the encryption algorithm, to generate the second encryption information, and the second decryption unit performs, on the decryption functional value and the second encryption information, subtraction as the decryption algorithm, to generate the decryption seed value," and, "the shared key generation apparatus performs, on the functional value and the seed value, multiplication as the encryption algorithm, to generate the second encryption information, and the second decryption unit performs, on the decryption functional value and the second encryption information, division as the decryption algorithm, to generate the decryption seed value." However, Hoffstein does

disclose a plurality of algorithms, equations, and/or formulas showing examples of methods of calculations that can be performed to successfully enable encryption in the disclosed invention. Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include the features disclosed by Hoffstein for the purposes of successfully enabling encryption in the invention.

Response to Arguments

5. Applicant's arguments filed 04/19/2007 have been fully considered but they are not persuasive.

Regarding application's Claim Objection argument(s):

- The applicant has used the term "conform" in similar contexts in Claims 10, 12, & 43, hence, the objection is maintained for consistency and usage of the term "conform" in its context.

Regarding applicant's Double Patenting arguments:

- Applicant's arguments regarding Claim 1 are not persuasive since a blind value or seed value may be used as a form of verification value and the number of units is independent of the actual method of invention. That is, regardless the number of components (e.g. first, second, third, etc) if the process is the same then there may be any number of components that perform those steps. The applicant's further argument regarding a first decryption unit and second decryption unit operable to decrypt first/second encryption information based on the first decryption verification value to generate a decryption seed value is an example of how the number of components is independent of the actual

method. Hence, the disclosure of Claim 1 of application '208; a decryption unit operable to decrypt the encryption information to generate a decryption seed value is equivalent to the disclosure of Claim 1 of the present application. The applicant's arguments regarding a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted is not persuasive since re-encryption information may be the same as the verification values. The same point regarding a multiple of components, as stated above, also applies to this argument.

- Applicant's arguments regarding Claim 3 are not persuasive since a verification value may very well be the same as a seed/blind value and vice versa. From this perspective, the two applications' ('102 and '208) would be identical in light of Claim 3.
- Applicant's arguments regarding Claim 24 are not persuasive since a verification value may very well be a seed value and vice versa. In addition, the verification values for determining whether a decryption shared key should be outputted may be information such as encryption information and/or re-encryption information.
- Applicant's arguments regarding Claims 46 & 47 are not persuasive since a verification value may very well be a seed/blind value and vice versa.
- Applicant's arguments regarding Claims 49 & 50 are not persuasive since a verification value may very well be a seed value which may be used twice for verification purposes in encryption/decryption. In addition, verification values may very well be encryption information and/or re-encryption information.

Regarding applicant's 35 U.S.C. 102(b) & 35 U.S.C. 103(a) arguments:

- Applicant's arguments regarding Claim 1 are not persuasive since the first shared-key generating unit and the second shared-key generating unit may be the same component/unit, in this case Dan. The applicant is also reminded that explicit citation of portions of a reference are for the applicant's convenience and are in no way supposed to limit the scope of the reference in the rejection. The examiner notes that the purpose of citing pages 18-19 were to show that Dan does require decoding/decryption information based on the calculations as disclosed earlier in the reference in order to decode/decrypt information received from Cathy. Dan performs polynomial calculations which implies that there is embedded verification information through the use of these formulas. That is, if the calculations do not result in an expected value then failure of decryption or generation of information would result. Thus, the results of the calculations for encryption/decryption and generation of a shared-key would be equivalent to verification values. In regards to the applicant's argument in light of a seed-value generating unit operable to generate a seed value; and a second encryption unit operable to encrypt the seed value based on the verification value, to generate second encryption information, the applicant is again reminded that explicit citation of portions of a reference are for the applicant's convenience and are in no way supposed to limit the scope of the reference in the rejection. Therefore, the seed-value generating unit and second encryption unit may be the same entity/component/element Dan and the explicit disclosure of Cathy was meant to show the interaction and functions of Dan, not as a limiter of the scope of the reference through a direct and narrow parallel comparison. Through the polynomial calculations, Dan generates a decryption seed value from the second encryption

information since the seed values inserted into the polynomial formulas must be correct in order for decryption to succeed, resulting in a verification. This implies that the result(s) from the calculations are verification values, and decryption seed values would be the successful result of polynomial calculations, permitting the decryption of information. Regarding the applicant's arguments pertaining to block 2 of Fig 2 failing to show a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether decryption shared key should be outputted, Fig 2 refers to Fig 3 which shows a simplified version of the procedure performed with polynomial calculations where unless the outcome(s)/result(s) of the polynomial calculations are as expected, decryption will not occur. The results of these calculations would be the verification values.

- Applicant's arguments regarding Claim 24 are not persuasive for at least similar reasons as discussed above with respect to Claim 1.
- Applicant's arguments regarding Claims 49 & 50 are not persuasive for at least similar reasons as discussed above with respect to Claim 1.
- Applicant's arguments regarding Claims 3-15, 18-23, 46, & 47 are not persuasive since in light of a seed-value generating unit operable to generate a seed value; and a second encryption unit operable to encrypt the seed value based on the verification value, to generate second encryption information, the applicant is again reminded that explicit citation of portions of a reference are for the applicant's convenience and are in no way supposed to limit the scope of the reference in the rejection. Therefore, the seed-value generating unit and second encryption unit may be the same entity/component/element

Dan and the explicit disclosure of Cathy was meant to show the interaction and functions of Dan, not as a limiter of the scope of the reference through a direct and narrow parallel comparison. Through the polynomial calculations, Dan generates a decryption seed value from the second encryption information since the seed values inserted into the polynomial formulas must be correct in order for decryption to succeed, resulting in a verification. This implies that the result(s) from the calculations are verification values, and decryption seed values would be the successful result of polynomial calculations, permitting the decryption of information.

- Applicant's arguments regarding Claims 46 & 47 are not persuasive for at least similar reasons as discussed above with respect to Claim 3.
- In regards to Claims 16, 17, 30, & 31 that depend from Claims 3 & 24, the 35 U.S.C. 102(b) rejection on Claims 3 & 24 are maintained, therefore, the rejection of their dependents is maintained.

Conclusion

6. Applicant's arguments filed 04/19/2007 have been fully considered but they are not persuasive.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
07/02/2007

Nasser Moazzami
Supervisory Patent Examiner